### DOCKET FILE COPY ORIGINAL

# Before the FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554

### RECEIVED

MAY 2 0 1998

FEDERAL COMMUNICATIONS COMMISSION

In the Matter of	)	OFFICE OF THE SECRETARY	¥
Communications Assistance for Law Enforcement Act	) ) )	CC Docket No. 97-213	

#### **COMMENTS**

#### BELLSOUTH CORPORATION

BELLSOUTH TELECOMMUNICATIONS, INC.

M. Robert Sutherland Theodore R. Kingsley Suite 1700 – 1155 Peachtree Street, N.E. Atlanta, GA 3030-3610 . (404) 249-3392 J. Lloyd Nault, II 4300 BellSouth Center 675 West Peachtree Street, N. E. Atlanta, GA 30375 (404) 335-0737

#### BELLSOUTH CELLULAR CORP.

BELLSOUTH PERSONAL COMMUNICATIONS, INC.

Michael P. Goggin Suite 910 – 1100 Peachtree St., N.E. Atlanta, GA 30309-4599 (404) 249-0919 Charles M. Nalbone Suite 400 – 3353 Peachtree Road, N.E. Atlanta, GA 30326 (404) 841-2017

#### BELLSOUTH WIRELESS DATA, L.P.

Michael W. White 10 Woodbridge Center Drive, 4<sup>th</sup> Floor Woodbridge, NJ 07095-1106 (732) 602-5453

May 20, 1998

No. of Copies reold Odd List ABODE

### TABLE OF CONTENTS

Summ	nary	i
1.	Introduction	1
II.	The Commission's Obligations Under CALEA Are Straightforward And Should Be Exercised Narrowly	3
III.	The Interim Industry Standard Complies With the Assistance Capability Requirements CALEA	
IV.	The FBI's Demands for Expansive New Surveillance Capabilities Should be Rejected: "Punch-List" Items	
V.	The CDT Objectives Would Further Delay CALEA Implementation at Substantial Additional Costs to Correct.	.16
VI.	The CTIA Petition Warrants Full Consideration By The Commission	.18
VII.	Conclusion	19

#### **SUMMARY**

The Commission should establish TIA interim technical standard J-STD-025 as the electronic surveillance technical standard to implement Section 103 of CALEA. The standard was forged by the industry over a three year process that included consultation with law enforcement and privacy interest groups and it provides law enforcement only those capabilities that Congress specified in the statute and its legislative history.

The FBI's so-called "punch list" items are designed to provide neither call identifying information nor communications content. The FBI/DOJ Petition therefore seeks extra-statutory features and functions that CALEA does not authorize. Moreover, technological complexity and expense render many of these items not reasonably available. CDT's deficiency petition relating to the provision of location and packet data is better reasoned, but fails to overcome the consensus solution achieved by industry. Concerns with respect to privacy rights in these contexts are appropriately addressed in individual cases by the interim standard, which allows carriers to suppress location information unless otherwise ordered by a court or other competent legal authority, and by a requirement that law enforcement extract addressing information only from packet data.

The CTIA Petition constitutes an accurate account of the history of the standard setting process. Its technological assessment of the assistance capability provisions of the industry consensus document is relevant to the pending proceeding because the consensus document was ultimately adopted as interim standard J-STD-025. The CTIA Petition warrants full consideration by the

Commission until it resolves the pending deficiency petitions and until it determines how to proceed with carrier requests for an extension of the CALEA compliance date.

# Before the FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554

In the Matter of	)	
Communications Assistance	)	CC Docket No. 97-213
for Law Enforcement Act	)	
	)	

#### **COMMENTS**

BellSouth Corporation, BellSouth Telecommunications, Inc., BellSouth Cellular Corp..

BellSouth Personal Communications, Inc., and BellSouth Wireless Data, L.P., ("BellSouth") on behalf of themselves and their affiliated companies, by counsel file these comments addressing (1) the issues raised concerning the scope of the assistance capability requirements necessary to satisfy the obligations imposed by the Communications Assistance for Law Enforcement Act ("CALEA"); and, (2) the Joint Motion to Dismiss CTIA's July 16, 1997, Petition for Rulemaking filed by the Department of Justice and the Federal Bureau of Investigation (FBI), pursuant to the Commission's Public Notice, DA 98-762, released April 20, 1998.

#### I. INTRODUCTION

For the past three and one half years, carriers and manufacturers have worked diligently through the Telecommunications Industry Association ("TIA") to develop a standard and adopt the electronic surveillance capabilities necessary to comply with Section 103 of CALEA. The results of these efforts, completed after lengthy delays detailed in the record in this proceeding,

Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in 18 U.S.C. and 47 U.S.C.).

Communications Assistance for Law Enforcement Act, CC Docket 97-213, Public Notice, DA 98-762 (released April 20, 1998) (Public Notice).

will permit the development and implementation of capabilities that fulfill the requirements of CALEA. On July 16, 1997, citing the obstructionist tactics of the FBI in orchestrating objections to the efforts of the TIA to adopt a standard, the Cellular Telecommunications Industry Association ("CTIA") petitioned the Commission to establish the then existing industry consensus document as the electronic surveillance technical standard pursuant to its authority under Section 107 of CALEA. When the Commission failed to act, the TIA adopted the proposed standard as interim standard J-STD-025. On March 27, 1998, the Department of Justice ("DOJ") and the Federal Bureau of Investigation ("FBI") jointly filed a petition asking the Commission to declare the interim standard deficient because it did not include certain enhanced surveillance capabilities the FBI desired. A day earlier, the Center for Democracy and Technology ("CDT") had filed a petition asking the Commission to declare the interim standard deficient because it allegedly does not adequately protect privacy.

BellSouth requests that the FCC establish J-STD-025 in its current form pursuant to Section 107. The FBI's insistence on using CALEA as a vehicle to require carriers to build technology into their systems to give law enforcement new, expanded surveillance capabilities flies in the face of Congress' intent that CALEA should merely ensure that, with the advance of telecommunications technologies, lawful surveillance capabilities should not be diminished. Some of the items the FBI demands are not reasonably achievable. Others go beyond what the law requires or permits. The CDT's objections, while more well-reasoned, would, if heeded, result in further delays in the implementation of CALEA and impose substantial additional costs on carriers.

# II. The Commission's Obligations Under CALEA Are Straightforward And Should Be Exercised Narrowly

Congress has defined the Commission's role regarding CALEA. The Commission's CALEA implementation obligations specifically are limited by Congress to the following: 1) to establish by rule, on the record, any technical requirements or standards necessary to implement the assistance capability requirements of CALEA; 2) to review and rule on petitions for extension of time to comply with the assistance capability requirements pursuant to Section 107; 3) to rule on petitions seeking a determination of "reasonably achievable" for equipment, facilities, and services installed or deployed after January 1. 1995; 3 4) to rule on carrier petitions to recover costs expended for making modifications to equipment, facilities, or services to make available the assistance capability requirements of Section 103; and, 5) to prescribe such rules as are necessary to implement the requirements of CALEA including rules to ensure that carriers implement electronic surveillance only in response to an appropriate court order or other lawful authorization. 4

The Commission must necessarily be guided in fulfilling its obligations under CALEA by the legislative history of CALEA. This legislative history clearly states the three purposes of the law: 1) to preserve (not enhance) government electronic surveillance capabilities; 2) to protect the privacy of customer's communications; and, 3) to not impede the industry's development and

BellSouth believes that once the full costs of industry compliance with the FBI's "requirements" which are outside the scope of CALEA, and other matters such as the deployment of capacity, are fully quantified, a number of carriers will be seeking appropriate relief under Sections 109(b) and 229(e) of CALEA.

Communications Assistance for Law Enforcement Act, CC Docket 97-213, Notice of Proposed Rulemaking (October 10, 1997) at 18, 25.

deployment of new technology, features, or services.<sup>5</sup> The Commission must also be mindful that Congress expected the telecommunications industry, the government, and the Commission to narrowly interpret CALEA and its requirements.<sup>6</sup> Thus, Congress stated in Section 107 (b) that should the Commission establish technical requirements or standards by rule, these rules must:

- 1. meet the assistance capability requirements of Section 103 by cost effective methods;
- 2. protect the privacy and security of communications not authorized to be intercepted;
- 3. minimize the cost of such compliance on customers:
- 4. serve the policy of the United States to encourage the provision of new technologies and services to the public; and,
- 5. provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the assistance capability requirements obligations of telecommunications carriers during any transition period.<sup>7</sup>

CALEA was enacted October 25, 1994, with its assistance capability and capacity requirements expected to be effective and available four years later on October 25, 1998. At least four critical events have occurred since the enactment of CALEA which have affected the ability of industry to comply with the law. First, the FBI has occasioned delays in several critical areas of implementation of the law including its delay of the industry standard setting process and its release of a final capacity notice which was almost three years late. Second, the Telecommunications Act of 1996 has changed the competitive environment in the industry as

<sup>&</sup>lt;sup>5</sup> H.R. Rep. No. 103-827, 103d Cong., 2d Sess., Pt. 1 at 9,13 (1994) (H.R. Rep. No. 203-827).

<sup>&</sup>lt;sup>6</sup> H.R. Rep. No. 103-827 at 22-23 (1994).

<sup>&</sup>lt;sup>7</sup> See 47 U.S.C. § 1006(b).

evidenced by many new entrants. Third, only approximately 100 million of the 500 million dollars authorized for cost reimbursement for CALEA has actually been appropriated even as Congress completes the last fiscal year of the authorization. Finally, virtually all carrier equipment and facilities currently being deployed in carrier networks are the same equipment and facilities which were being deployed prior to January 1, 1995, since the technology to make them "CALEA capable" has not yet been developed nor designed into such equipment and facilities.

The \$500 million authorized to be appropriated will be woefully insufficient to reimburse the industry for its costs of compliance with CALEA and thus be inadequate to achieve the FBI's desired level of compliance. In apparent recognition of this fact, the FBI has attempted to creatively interpret and implement CALEA in such a fashion that significant unreimbursed costs are expected to be passed on to the industry and its customers. It is against this backdrop that the Commission undertakes the unenviable task of providing some certainty and appropriate guidance to the telecommunications industry as it seeks to implement CALEA. The Commission must implement CALEA as it was intended by Congress; that is, narrowly and in a cost-effective fashion.

## III. The Interim Industry Standard Complies With the Assistance Capability Requirements of CALEA

Interim industry standard J-STD-025 is designed to enable carriers to comply with the assistance capability requirements of CALEA set forth in Section 103.<sup>8</sup> Under Section 103 carriers must ensure that their networks can do the following:

The Comments of the Telecommunications Industry Association (TIA) have previously detailed for the Commission the industry's good faith compliance efforts in the implementation of CALEA, and the 3 year effort to develop technical standards and address law enforcements electronic surveillance concerns. See comments at 14-18.

- 1. Isolate expeditiously the *content* of the subject's or target's *communications*.
- 2. Isolate expeditiously the originating and destination numbers (*call identifying information*) of the targeted communications, but not the physical location of the target.
- 3. Provide such intercepted *communications* and *call identifying information* to law enforcement and;
- 4. Carry out communications interceptions unobtrusively so that the targets of electronic surveillance are not aware of such interceptions and so that the privacy and security of other communications are not compromised.<sup>9</sup>

Much of the debate between industry and law enforcement has focused on defining that which carrier networks are to be enabled to deliver to law enforcement pursuant to a valid court order or other lawful authorization. It is clear from the express language of the statute<sup>10</sup> and its legislative history,<sup>11</sup> that Congress intended for the assistance capability requirements for telecommunications carriers to be limited to the provision of communications "content" and "call identifying information" to law enforcement. The meaning of the *content* of a surveillance subject's or target's *communications* is obvious. However, Congress chose to define the term *call identifying information* in CALEA in order to clearly specify that such information is limited to "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." Thus, with respect to intercepted voice communications, call identifying information would typically be the:

"electronic pulses, audio tones, or signaling messages that *identify the numbers* dialed or otherwise transmitted for the purpose of routing calls through the

<sup>&</sup>lt;sup>9</sup> 47 U.S.C. § 1002; H.R. Rep. No. 103-827 at 16. (emphasis added)

<sup>&</sup>lt;sup>10</sup> 47 U.S.C. §§ 1001, 1002.

H.R. Rep. No. 103-827 at 21.

<sup>&</sup>lt;sup>12</sup> 47 U.S.C. § 1001.

telecommunications carriers network. In pen register investigation, these pulses, tones, or messages *identify the numbers* dialed from the facility that is the subject of the court order or other lawful authorization. In trap and trace investigations, these are the incoming pulses, tones, or messages which *identify the originating number* of the facility from which the call was placed and which are captured when directed to the facility that is the subject of the court order or authorization. Other dialing tones that may be generated by the sender that are used to signal customer premises equipment of the recipient are not to be treated as call identifying information." (emphasis supplied)<sup>13</sup>

Thus, Congress defined "call identifying information" narrowly to include only numbers, that is, only the dialing or signaling information of the targeted communication which identifies the originating and destination numbers, not other carrier network messages, tones, signals or information. Further, the legislative history is unequivocal that the communications content and call identifying information which carriers must provide to law enforcement must be *reasonably* available to the carrier. <sup>14</sup>

In light of the plain words of CALEA and Congress' intent in enacting the law as reflected in the legislative history, it is obvious why the industry standards group rejected the FBI's so-called punch list as beyond the scope of the assistance capability requirements of CALEA. The features and capabilities sought by the FBI in its punch list do not constitute either the "content of communications" or "call identifying information". Furthermore, many of them are not reasonably available to carriers.

# IV. The FBI's Demands for Expansive New Surveillance Capabilities Should be Rejected: "Punch-List" Items

In their petition, the DOJ and FBI insist that the Commission establish a standard that would force manufacturers to develop, and carriers to purchase, intrusive, expensive, capabilities

H.R. Rep. No. 103-827 at 21.

H.R. Rep. No. 103-827 at 22.

that would greatly expand the scope of the FBI's electronic surveillance capabilities. In some cases, the features the FBI would mandate are simply not reasonably achievable or available. In others, the FBI's demands simply go beyond what the law requires or permits. In all cases, the FBI simply fails to establish that CALEA (or any other statute) requires such an expansion of surveillance capabilities. The industry standard is not deficient because the items listed in Appendix I "Proposed Final Rule" of the FBI/DOJ Petition are neither communications content nor call identifying information as those terms are used in CALEA and its legislative history. Further, in some cases, the item is not reasonably available to carriers.

- (a) All Content of Conferenced Calls. The FBI/DOJ Petition concedes that the TIA interim standard "does not amount to a reduction in the information that has been available to law enforcement". This concession is dispositive. For although the FBI/DOJ Petition purports to argue that that TIA interim standard nevertheless "falls short of carrying out the legal obligations imposed by Section 103 of CALEA," the FBI Director has testified before Congress that CALEA was "intended to preserve the status quo, that it was intended to provide law enforcement with no more and no less access to information than it had in the past." The TIA interim standard correctly implements CALEA's requirement that it is the communications content of the specific target, or subject, of the authorized electronic surveillance which is at issue.
- (b) Party Hold, Party Join, and Party Drop Messages. The FBI/DOJ Petition argues that exclusion of messages indicating which parties are added to or dropped from a call "will

Joint Petition for Expedited Rulemaking, Federal Bureau of Investigation and Department of Justice (March 27, 1998) at 30 (FBI/DOJ Petition).

ld.

H.R. Rep. No. 103-827, at 22-23 (1994).

deprive law enforcement of important investigative and evidentiary information." CDT correctly argues that such "messages do not relate to call-identifying information but rather seek to enhance law enforcement investigative techniques beyond the status quo." As demonstrated in Section III above, the actual call-identifying information intended by Congress is simply the number indicating call origination or destination. This is true regardless of whether the medium is electronic pulses (such as dial pulses), audio tones (such as touch-tones or MultiFrequency tones), or signaling messages (such as ISDN D-channel messages). Information such as which parties are on a call (or indications such as dial tone, lights, busy tone or ringback tone) are clearly not "numbers" and therefore not call-identifying information. While information leading to the identity of third parties who join or drop from a target's call may be useful to law enforcement for any number of purposes, it is not information as to "call content" nor is it "call identifying." It is information that is beyond the scope of CALEA.

Moreover, the provision of party join, party drop and party hold messages would be extremely difficult to achieve. In all but the simplest cases, conference calls are established in a remote conferencing bridge, separate from the voice switch. This means that information about the status of parties to the conference is not readily available to the network element that normally interfaces with law enforcement, the switch. Recording and delivering information about the status of parties on a conference call would require either: (1) upgrades to conference bridges to make them intelligent devices capable of generating messages to law enforcement or, (2) the development and deployment of a separate message link between a conference bridge and

FBI/DOJ Petition at 42.

Petition for Rulemaking and Sections 107 and 109 of the Communications Assistance for Law Enforcement Act, Center for Democracy and Technology (March 16, 1998) (CDT Petition) at 14.

a switch to convey status information to the switch and subsequently to law enforcement. Thus, even if these messages could be considered "call-identifying information" for purposes of CALEA, to require their provision would be technically not feasible and not cost-effective..

messages indicating when a subject performed a switchhook flash or pressed a feature key should be included in J-STD-025 because such information is call-identifying information, and because historically law enforcement could tell when a switchhook was pressed when using an older analog pen register. Again, CDT demonstrates that such information is not call-identifying information. According to the interim technical standard J-STD-025, signaling information that relates to the origination or destination of a call, such as dialed digits, will be delivered to law enforcement. At issue are other stimuli on the subject's access line that do not have to do with the routing of a call. These stimuli are not call-identifying information under CALEA.

The FBI's argument that this information should be provided because it was detectable when pen registers were conducted in the days of analog technology is not persuasive. CALEA specifically requires carriers to provide call-identifying information "in a manner that protects the privacy and security of communications and call identifying information not authorized to be intercepted." Given this statutory imperative, the Commission must reject the Joint Petitioners' claim that carriers have an obligation under CALEA to develop capabilities to provide

FBI/DOJ Petition at 36-36.

CDT Petition at 14.

<sup>&</sup>lt;sup>22</sup> 47 U.S.C. 103(a)(4)(A).

information that does not fall within the CALEA definition of "call-identifying information" simply because the information may have been detected by the FBI in the past. Where new technology enables precision implementation of the intent of the law with regard to the protection of privacy interests, new technology must be utilized to do so. Past technological limitations should not dictate that new implementations deliver information not specifically authorized by Congress.

There are also technical issues which can make this capability difficult and expensive to achieve. In some switch implementations, detection and collection of off-hook and digits occurs in a line module which is separate and distinct from the main processor of the switch. The processor of the switch is not involved unless a valid digit pattern is collected. Making this information available to the main processor so that it can be sent to law enforcement may require fundamental modifications to a switch architecture that are not reasonably achievable. Thus, even if such information could be considered "call-identifying information", as the FBI erroneously asserts, the technology is not reasonably available.

(d) Notification Messages for In-band and Out-of-band Signaling. The FBI/DOJ Petition argues that indications of network-generated in-band and out-of-band signaling should be included in J-STD-025 because such information is call-identifying information.<sup>23</sup> Again, the CDT demonstrates that such information is not call-identifying information.<sup>24</sup> In addition, there are serious technical issues with providing this information. In the case where a tone or indication is generated by the local switch, a message reporting the tone or indication would usually be redundant. For example, in the case where a subject is on the phone and there is

FBI/DOJ Petition at 45-47.

<sup>&</sup>lt;sup>24</sup> CDT Petition at. 14.

another incoming call attempt, it can be easily inferred from knowledge of normal call processing that either the calling party hears busy tone, or (if the subject has call waiting) the calling party hears ringback and the subject hears a call-waiting tone. Paying the cost for software upgrades that would generate a set of messages to convey redundant information makes no sense, and is not sanctioned by CALEA.

In the case where tone or other indication is generated in a different switch from the one serving the subject, not only would the information be mostly redundant, but capability would need to be added at the local switch to detect all possible tones or indications that could be returned over a connection to a remote switch. For example, if a subject calls a party on another switch or network, the subject's local switch would need to be able to detect busy tone, reorder tone, ringback, etc. that may be present on the connection in order to be able to inform law enforcement of this fact. Such modifications would place a heavy burden on network providers, and provide practically no functionality over that which can already be inferred from a knowledge of how a normal call is processed. Thus interim standard J-STD-025 is correct as it stands and this capability should not be added.

that timing requirements for delivery of information should be included in J-STD-025. This topic was discussed extensively in the standards organization during the development of J-STD-025. Law enforcement was informed by telecommunications industry participants that call-identifying information would be delivered over the Call Data Channel in a timely manner, but that normal switch call processing must be the first priority in order to maintain the present level of service for customers. In addition, network switches are not presently synchronized to

FBI/DOJ Petition at 49-52.

Universal Coordinated Time (UCT) and such coordination would represent a considerable expense. Establishing an arbitrary timing requirement, without a thorough knowledge of how CALEA will be implemented or how law enforcement will choose to transport channels, is inappropriate. Interim standard J-STD-025 is therefore correct as it stands and this requirement should not be added.

- status capability should be included in J-STD-025. The standards organization chose not to standardize a surveillance status message because it only makes sense in certain distribution architectures, e.g., when only a single switch is involved in the surveillance and the status of the one element of the surveillance can be readily verified. For this purpose, an optional Connection Test Message was included in J-STD-025 in Annex E. For networks like cellular networks in which the surveillance is necessarily distributed, or in cases where a distribution box is used to consolidate content and call identifying information from several network elements and deliver it simultaneously to multiple law enforcement collection sites, it is impossible to verify the status of all elements and create a valid surveillance status message. In any event, surveillance status message is not call identifying information, because its implementation in certain types of networks is not "reasonably achievable".
- (g) <u>Feature Status Message</u>. The FBI/DOJ Petition argues that the ability to automatically report changes in a subject's features and services should be included in J-STD-025.<sup>27</sup> The CDT argues that such information is currently provided by subpoena, and "would be a significant precedent requiring carriers to generate a type of on-line customer service profile

FBI/DOJ Petition at 52-55.

FBI/DOJ Petition at 56-57.

solely for the benefit of government surveillance." This information is obviously not call identifying information since it has nothing to do with the origin or destination of a call. Law enforcement claims that the information is necessary to allow a determination of the number of delivery channels required. In actuality, using information about services subscribed to by a subject to determine delivery requirements is a useless exercise in today's environment.

BellSouth widely offers on-demand services such as call forwarding, three way calling, and call return. A subject can access these services at any time without a subscription. Since the time required to add additional channels will be at least a day or so, law enforcement will need to assume that the on-demand services will be used in order to properly size the number of delivery channels. Thus, the number of channels required for subjects who subscribe to services and those who have them available on-demand will be the same.

Additionally, the trend in telecommunications is toward distributing service logic and service profile information, as exhibited by the growth of Advanced Intelligent Network ("AIN") Services. In such a distributed network, requiring carriers to implement technology to deliver service status and service profile information from a multitude of various distributed network elements would be an onerous requirement, and could stifle the growth of new and innovative services.

(h) <u>Continuity Check</u>. The FBI/DOJ Petition argues that a requirement for a continuity tone on dedicated content channels should be included in J-STD-025.<sup>29</sup> The standards organization chose not to include continuity checks in the body of the standard, but rather to include information about continuity checks in an informative annex, since it recognized that

<sup>&</sup>lt;sup>28</sup> CDT Petition at 14.

FBI/DOJ Petition at 54.

several types of content delivery could possibly be utilized. The tone continuity check proposed in the FBI/DOJ Petition is appropriate only when dedicated content channels are provided. BellSouth supports the use of a continuity tone if its use is limited to instances where dedicated content delivery channels from the switch to LEA locations are involved. Otherwise the ability to provide this feature (over a switched channel) is technically not feasible and should not be required.

(i) <u>Dialed Digit Extraction</u>. The FBI/DOJ Petition argues that a requirement that a carrier's equipment should extract dialed digits and inform law enforcement over the Call Data Channel should be included in J-STD-025.<sup>30</sup> The CDT argues that the local carrier cannot determine whether post cut-through digits are call identifying or not, and that law enforcement should serve the carrier that actually processes the number (e.g., a long distance carrier) with a pen register order.<sup>31</sup> Law enforcement should be required to install and utilize equipment to extract addressing information as set forth in 18 U.S.C. § 3121(c).

In the development of J-STD-025, the discussions about this feature were mainly technological and economic. For normal call processing, touch tone digits are detected by a touch tone register since the touch tone register is a shared resource, it is only associated with a call for a short duration when dialing occurs, and is then made available for use by another call. Requiring this shared resource to monitor a call for its entire duration (as would be needed to detect any post cut-through digits) could impact the level of service for other customers in an office. In addition, some technologies (such as cellular and PCS) may not presently have the ability to detect touch tones at all, relying on out-of-band signaling messages to process calls.

FBI/DOJ Petition at 38-42 and 47-49.

CDT Petition at 13.

The standard assumes the ability of law enforcement to use a call content channel to monitor the transmit (i.e. content being transmitted) from a subject, and to identify and record any post cut-through dialed digits. This removes the uneconomical necessity to deploy additional touch tone registers in all switches across the nation just to accommodate law enforcement, and also relieves the local carrier of any decision as to whether or not digits are intended as call routing.

(j) <u>Ceiling Limit on Number of Interfaces</u>. The FBI/DOJ Petition argues that a limited set of standard delivery protocols should be included in J-STD-025.<sup>32</sup> The standard requires that call content and call identifying information be delivered over a standard, or widely used interface. A list of possible protocol stacks is provided in J-STD-025, Annex A. Specific requirements were not imposed on supplier's equipment in recognition that such requirements might result in a fundamental redesign of existing equipment at considerable expense. A conversion of the protocol can be done at a collection site at much less cost than modifying existing equipment.

## V. The CDT Objectives Would Further Delay CALEA Implementation at Substantial Additional Costs to Correct.

The CDT Petition cites two specific instances where the CDT feels that J-STD-025 goes beyond the requirements of CALEA, and in fact violates the mandate to preserve the privacy and security of communications. <sup>33</sup> The first instance deals with the delivery of location information by cellular and PCS providers when a call is originated from, or terminated to, an intercept subject. While location arguably falls outside of the strict definition of call identifying information, the TIA T.R45.2. standards organization agreed to provide location in this limited

FBI/DOJ Petition at 57-58.

CDT Petition at 8-10.

case as an accommodation to law enforcement. The J-STD-025 protocol, however, identifies location as "Conditional" information in all cases, meaning that certain conditions must be met before it is provided. In the case of location the conditions are "the location information is reasonably available . . . and delivery is authorized". Thus, the carrier should have the ability to suppress location information, and it should do so unless the court order for the surveillance specifically authorizes its delivery.

Second, the CDT argues that J-STD-025 is deficient in its handling of packet data. The standard allows for delivery of packet data messages, in their entirety, to law enforcement. This capability is provided to allow carriers to comply with Title III court orders. The CDT argues that, for privacy reasons, a capability should be defined which would allow the delivery of addressing information extracted from the packet, while stripping out other portions of the packet. This capability would presumably be used in the case of a pen-register court order (although it is not clear that addresses contained inside packets are covered under the pen register statute). The standards organization chose to support delivery of packet content and call identifying information in the present manner for technical reasons. In the most common architecture in place today, packets are processed in a packet data handler, separate from the voice switch. This means that the addressing information is not readily available to the network element that normally interfaces to law enforcement, the switch. Even if the address information available to the carrier could be extracted, in most cases it is of local significance only, i.e., it is the address of a local server and the ultimate destination of the packet is contained in the content of the packet. In many cases the carrier is not aware of the protocol being transported and cannot determine the ultimate address. In the final resolution, J-STD-025 assumes that the full packet

<sup>&</sup>lt;sup>34</sup> J-STD-025

will be delivered to law enforcement and that law enforcement will determine the protocol being utilized in the packet content and the ultimate address. It is assumed that law enforcement will install equipment to do this functionality as it is authorized to do for pen registers.

#### VI. The CTIA Petition Warrants Full Consideration By The Commission

On March 27, 1998 the Department of Justice and the Federal Bureau of Investigation (FBI) moved to dismiss as moot the July 16, 1997 Petition for Rulemaking filed by the Cellular Telecommunications Industry Association (CTIA Petition). The FBI alleges that its own pending deficiency petition "supersedes CTIA's petition in terms of relevancy and accuracy." The pending FBI petition does not supersede CTIA's petition in terms of accuracy, and the CTIA Petition remains an important, timely and accurate part of the record in this proceeding. The CTIA Petition warrants careful consideration by the Commission as it considers all of the pleadings filed subsequent to July 16, 1997, even though its request to establish a rulemaking to establish a technical standard can be accommodated by the Commission's resolution of the pending FBI and CDT deficiency petitions.

Only one fact raised in the CTIA Petition is arguably moot; there can be no controversy that on December 8, 1997 the TIA adopted an interim technical standard which adopted, and hence superceded the earlier consensus document referred to in the CTIA Petition. But the consensus document is largely reflected in the current interim technical standard, and CTIA's comments on the sufficiency of the consensus document remain relevant to the pending challenges to the sufficiency of the interim technical standard. Furthermore, the salient point of the CTIA Petition, that "the TIA standards process will not yield a standard in sufficient time to

Joint Motion to Dismiss CTIA's July 16, 1997, Petition for Rulemaking, Department of Justice and Federal Bureau of Investigation (March 27, 1998) (FBI Motion).

permit industry-wide implementation by the October 1998 compliance deadline,"<sup>36</sup> remains as accurate and relevant today as ever. The fact that an interim standard was published in December of 1997 does not change this fact. The CTIA's complete discussion of the background of the standard setting process is comprehensive and accurate and should be considered by the Commission as it considers all of the pleadings in this proceeding.

Accordingly, the Commission should not grant the FBI Motion until it issues a final order terminating the CDT and FBI deficiency petitions, and resolves how it will handle extensions of the CALEA compliance data. In the meantime, it should refer to the CTIA Petition for essential background information and for relevant analysis of industry efforts to adopt a CALEA-compliant technical standard.

#### VII. CONCLUSION

For the forgoing reasons, the Commission should dismiss the FBI/DOJ and CDT Petitions, establish TIA interim technical standard J-STD-025 as the electronic surveillance technical standard to implement Section 103 of CALEA, toll the CALEA compliance date pending release of its final order, and grant all affected carriers a blanket extension of the

19

CTIA Petition at 11.

October 25, 1998 compliance date for a period of not less than two years from the final effective date of the newly adopted technical standard.

Respectfully submitted,

INC.

BELLSOUTH TELECOMMUNICATIONS, IN
By: Royal Royal Tault I
I. Lloyd Nault, II JEC
4300 BellSouth Center
N.E. 675 West Peachtree Street, N. E.
Atlanta, GA 30375
(404) 335-0737
BELLSOUTH PERSONAL
COMMUNICATIONS, INC.
By: Charle M Wallone
Charles M. Nalbone
Suite 400 – 3353 Peachtree Road, N.E.
Atlanta, GA 30326
(404) 841-2017
oor

May 20, 1998

### **CERTIFICATE OF SERVICE**

I hereby certify that I have this 20th day of May 1998, serviced all parties to this action with the foregoing COMMENTS, reference docket CC 97-213, by hand service or by placing a true and correct copy of the same in the United States Mail, postage prepaid, addressed to the parties as set forth on the attached service list.

Iulia W Spires